

Enhancing the effectiveness of CAPTCHA using an improved visual cryptography scheme

Chihi Hasnae, Chahboun Asaad

Abdelmalek Essaadi University, National School of Applied Sciences of Tangier (ENSAT),
Mathematics and Intelligent Systems Team (MASI), ENSA Tanger, Tanger principale, Morocco

Article Info

Article history:

Received Jan 12, 2025

Revised Apr 9, 2025

Accepted Jul 2, 2025

Keywords:

Authenticate phase

Captcha

Registration phase

Spamming

Visual cryptography

ABSTRACT

Traditional CAPTCHA systems, designed to distinguish humans from bots, are increasingly ineffective due to advancements in artificial intelligence (AI), particularly deep learning and optical character recognition (OCR) technologies, which enable bots to bypass these systems. This paper proposes a new CAPTCHA authentication method that combines enhanced visual cryptography with traditional techniques to improve security. Visual cryptography divides information into visually distinct shares, reinforcing CAPTCHA's defenses against automated attacks, especially those using deep learning. This approach not only strengthens security but also improves user experience by adjusting the time required to complete CAPTCHA challenges, addressing usability concerns associated with traditional systems. Overall, the proposed method offers a more secure, efficient, and user friendly solution for online authentication.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Chihi Hasnae

Abdelmalek Essaadi University, National School of Applied Sciences of Tangier (ENSAT)

Mathematics and Intelligent Systems Team (MASI), ENSA Tanger

Tanger principale, Morocco

Email: chihi.hasnaa@gmail.com

1. INTRODUCTION

CAPTCHAs have become essential security tools, these tests are used to differentiate automated bots from human users on websites, they present tasks that are easily solvable by humans but pose significant challenges to machines (Figure 1). For example, users may be asked to identify distorted characters, select specific objects in images, or complete simple puzzles [1]-[5]. The primary function of CAPTCHAs is to block automated bots from scraping sensitive data, account hijacking and spamming.

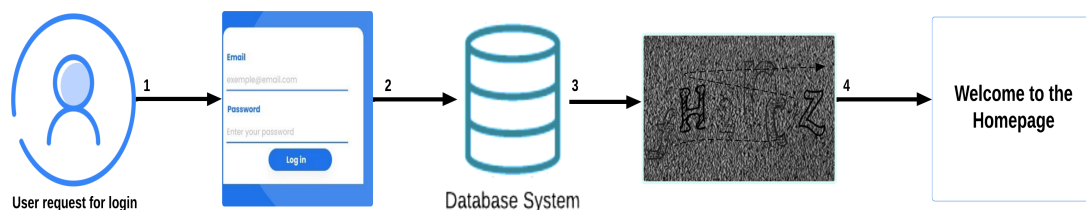


Figure 1. CAPTCHA for authentication

Text based CAPTCHAs are typically generated by taking text and applying various alterations such as distortion, noise, broken letters or warping. These modifications are intentionally added to make the text difficult for automated systems, like bots, to interpret, while still remaining legible to human users. By incorporating these elements, CAPTCHAs effectively distinguish between human users and machines, ensuring that only humans can successfully complete the task [6], [7]. To be deemed secure, a CAPTCHA must maintain an extremely low chance of being solved by automated tools, specifically, less than 0.0001%, while also ensuring that at least 80% of human users can successfully read and complete it [7].

As machine learning and AI technologies progress, CAPTCHAs must adapt to counter increasingly sophisticated bot strategies. This ongoing need for innovation has led to the development of more complex CAPTCHA methods, including image recognition challenges, puzzle based CAPTCHAs and behavioral analysis techniques, to maintain a high level of security while ensuring user accessibility [6], [7]. Other methods have been developed on non-Latin languages, such as Hindi, Chinese, or Arabic languages (see [8]-[11]).

Moreover, visual cryptography is a sophisticated cryptographic method developed to enhance the security of image transmission by encoding them into multiple shares. Each share is essentially a fragment of the original image, and the method ensures that no complex decryption algorithms are required. Naor and Shamir's groundbreaking work in 1994 [12] introduced the (k, n) -threshold scheme, in which an image is divided into n parts. The original image can be reconstructed visually by combining any k or more shares, whereas fewer than k shares reveal no information about the image, preserving its confidentiality. This scheme was initially designed for black and white images, but over time, it has been extended to support color images, broadening its scope and utility. The approach offers robust protection against unauthorized access by preventing any single share from revealing valuable information, thus enhancing security. Moreover, it is computationally efficient, as it allows for easy visual reconstruction, even without sophisticated algorithms or hardware, making it particularly valuable for practical applications.

Visual cryptography is increasingly being used to enhance CAPTCHA systems by adding an additional layer of security through image based challenges. Traditional CAPTCHA tests typically involve distorted text that users must decipher, but visual cryptography introduces a method where the challenge is based on splitting an image into multiple parts, making it difficult for automated bots to decipher. In this system, an image is divided into two or more shares, and only when combined correctly by the human user does it reveal the original image or message. This technique effectively prevents bots from passing the CAPTCHA, as they struggle to process visual patterns in the same way humans do. By leveraging visual cryptography, CAPTCHA systems can provide a more robust defense against automated attacks, ensuring a higher level of security for online platforms [13].

This article provides a comprehensive analysis of the integration of an advanced visual cryptography system within CAPTCHA mechanisms, aimed at enhancing the efficiency of online validation processes. The proposed system not only strengthens the security of the CAPTCHA framework by making it more resilient to automated attacks but also offers significant adaptability in validation speed. Compared to traditional CAPTCHA systems, this enhanced approach adjusts the time required for users to complete the validation process, resulting in a more streamlined and efficient user experience. Importantly, these efficiency gains are achieved without compromising the underlying security, thereby maintaining the integrity of the CAPTCHA as a reliable tool for distinguishing human users from automated bots.

2. ENHANCED VISUAL CRYPTOGRAPHY

Visual cryptography is an advanced cryptographic technique designed to bolster the security of image transmission by encoding images into multiple shares, each representing a partial fragment of the original. This technique eliminates the need for complex decryption algorithms, as the image can be reconstructed through the visual alignment of the shares. The seminal work of Naor and Shamir in 1994 [12] introduced the (k, n) -threshold scheme, in which an image is divided into n parts. The original image can be reconstructed by combining any k or more shares, while fewer than k shares provide no information, ensuring the image's confidentiality. Initially developed for black and white images, this method has since been extended to accommodate color images, thereby expanding its applicability. The scheme offers strong protection against unauthorized access by ensuring that no single share contains sufficient information to reconstruct the image. Furthermore, its computational efficiency makes it highly practical, as it allows for straight forward visual reconstruction without the need for complex algorithms or specialized hardware, making it an attractive solution for various real world applications.

Numerous methods have been proposed for constructing visual cryptographic schemes based on matrices, where the columns of a given weight appear with same prevalence [14]-[16]. Adhikari [17] introduced new visual cryptographic systems, applying linear algebraic techniques to both monochrome and color images. Liu *et al.* [18] utilized a recursive approach involving a $(2, 2)$ -VCS within a construction tree framework, which generates a VCS for both OR and XOR cases.

A critical challenge in visual cryptography schemes (VCS) is achieving high contrast while minimizing pixel expansion. Explicit constructions of contrast optimal basis matrices, particularly for smaller values of k , are presented in [19]. Additionally, the optimal contrast values' upper and lower bounds have been thoroughly examined in several studies [19]-[22]. Various methods to optimize relative contrast have been explored [23], where the contrast maximization problem is addressed as a linear programming issue.

A (k, n) VCS is a type of secret sharing scheme where a secret (typically an image or visual data) is divided into n shares, and the secret can only be reconstructed when at least k of those shares are combined. The key feature of a (k, n) scheme is that each share, when viewed individually, appears as random noise and reveals no information about the secret. However, when at least k shares are overlaid or combined, the original secret can be fully reconstructed.

Consider the scenario where the secret image consists only of black and white pixels. Let S represent a Boolean matrix with size $n \times m$, and let $Y \subseteq \{1, \dots, n\}$. We denote by $S[Y]$ the submatrix of S consisting of rows indexed by the elements of Y , and this submatrix will have dimensions $|Y| \times m$. Additionally, S_Y represents the XOR operations applied to the rows of $S[Y]$. The number of ones in the row vector S_Y is called the Hamming weight and denoted by $w(S_Y)$.

In the following, we will modify this visual cryptography method to enhance the efficiency and applicability of the scheme in order to apply it on CAPTCHAs. The modified approach will allow for greater scalability and better integration with CAPTCHAs applications, offering a more robust solution for secure visual communication. The improved VCS will be defined as follows.

The binary matrices S^0 and S^1 , with size $n \times m$, are defined as the basis matrices of a (k, n) -VCS if for all subsets $Y \subseteq \{j_1, \dots, j_n\}$, either there is a positive real number $\alpha > 0$ such that,

$$w(S_Y^1) - w(S_Y^0) \geq \alpha m,$$

or the two $|Y| \times m$ matrices $S^0[Y]$ and $S^1[Y]$, formed by restricting S^1 and S^0 to rows indexed by $j_1, j_2, \dots, j_k$, are identical under column permutation.

Throughout the remainder of the paper, we will consider the following example of basis matrices.

$$S^0 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad S^1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

For all $Y \subseteq \{1, \dots, 4\}$ and considering the XOR operation, we summarize the computation of the Hamming weight of S_Y^1 and S_Y^0 associated with these two basis matrices in Table 1.

Table 1. The computation of the hamming weight of S_Y^1 and S_Y^0

The number of elements of Y	$w(S_Y^0)$	$w(S_Y^1)$
1	3	7
2	4	4
3	3	3
4	0	8

So, $w(S_Y^1) - w(S_Y^0) \geq \frac{4}{9} \times 9$ when Y has either one or four elements from $\{1, \dots, 4\}$, then the contrast is equal to $\frac{4}{9}$. In these cases, when we look at the shares visually or stack four of them, we will be able to visualize them and read their content. However, when we stack two or three shares, the resulting images are blurred and not clear at all.

3. THE PROPOSED METHOD

Contrary to the CAPTCHA method, for which the user must enter the text displayed in distorted images, our proposed method is based on the human ability to visualize text and determine whether it is readable or a distorted image. Unlike traditional systems that require specific tasks like solving puzzles or interpreting images, our approach leverages the innate skill of humans to distinguish between clear text and blurred or scrambled visuals. This enables us to create a more intuitive and seamless verification process, where users can easily identify and report whether the displayed content is legible, providing a highly effective barrier against automated bots without disrupting the user experience.

In the registration phase, the client submits their ID and password through a secure interface, which are then transmitted to the server. The server processes the data by securely storing the credentials in its database, using encryption methods to ensure that the sensitive information remains protected. The password is typically hashed before being stored, making it unreadable to unauthorized parties. Once the credentials are successfully recorded, the server may send a confirmation response to the client, indicating that the registration was successful. This step ensures that the client's login information is securely saved for future authentication attempts (Figure 2).

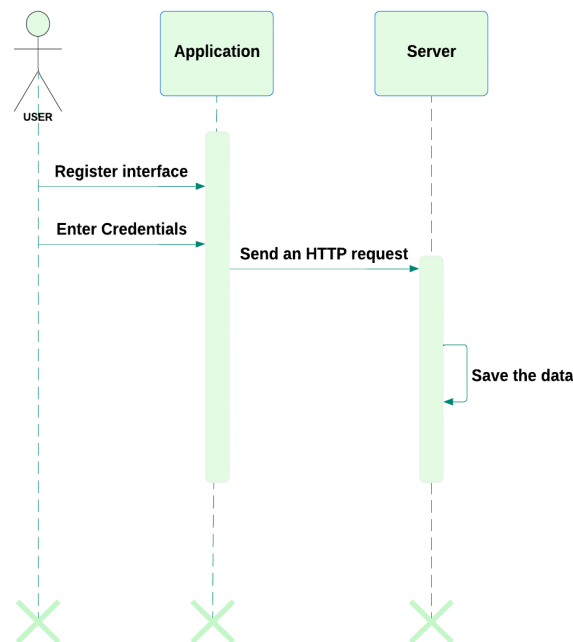


Figure 2. Registration phase

In the authenticate phase, the server sends the first share to the client. If the share is readable, the client clicks on “CAPTCHA” button; if the image is blurred and unreadable, the client does not click on “CAPTCHA” button (Figure 3).

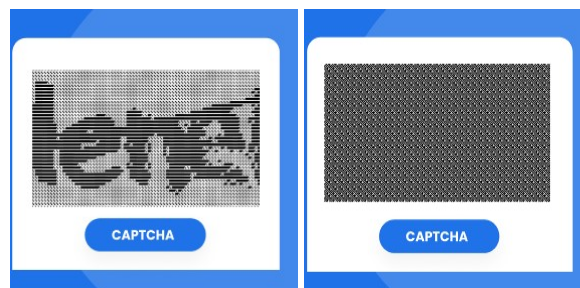


Figure 3. CAPTCHA button

The server in this case will receive the message “NOT CAPTCHA” from the client. The server then sends the second share, which will be stacked with the first share using the XOR operation. If the stacked image is readable, the client clicks on “CAPTCHA” button; if it remains unreadable, the client does not click on “CAPTCHA” button. The server proceeds by sending the third share, which is stacked with the previous image using XOR operation. If the newly stacked image is readable, the client clicks on “CAPTCHA” button; if it is still unreadable, the client does not click on “CAPTCHA” button. Finally, the server sends the last share, which will be stacked onto the image processed previously. If the resulting image is readable, the client clicks on “CAPTCHA” button; if it is unreadable, the client does not click on “NOT CAPTCHA” button and the server will receive the message “NOT CAPTCHA” in this case (Figure 4).

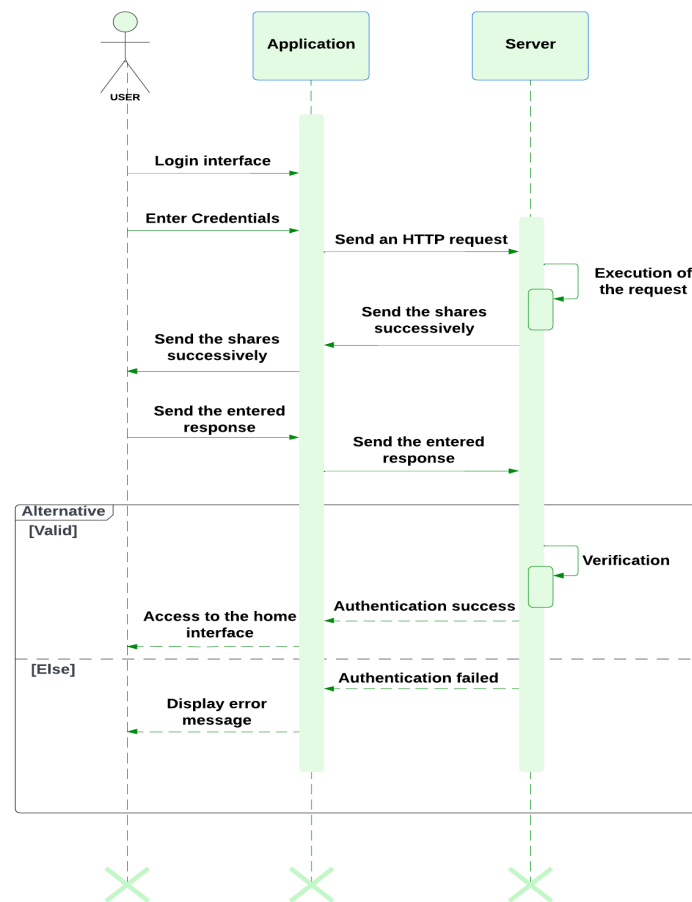


Figure 4. Authenticate phase

For example, using the textual CAPTCHA image “4gycb” and visual cryptographic scheme like the one described in Table 1. The server splits the CAPTCHA image “4gycb” into four shares, then it sends the first share to the client, and the received image is clearly readable, so the client clicks the “CAPTCHA” button. Then, the server sends the second share, which is stacked on the first one using the XOR operation. The resulting image is unreadable and distorted, so the client does not click on the “CAPTCHA” button. The server now sends the third share, which is stacked on the previous image, resulting in another unreadable and distorted image. The client does not click on the “CAPTCHA” button again. Finally, the server sends the last share to the client, which is stacked onto the previous image, and the result is readable by the client, who clicks the “CAPTCHA” button. Once the server receives the correct responses in the order “CAPTCHA-NOT CAPTCHA-NOT CAPTCHA-CAPTCHA,” it validates the connection and authentication with the client, allowing the client to access the server (Figure 5).

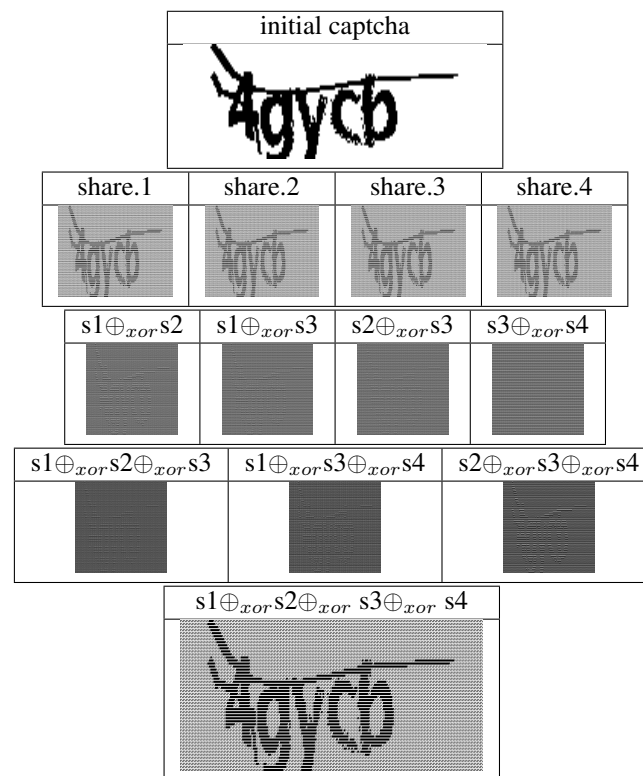


Figure 5. VCS applied to textual CAPTCHA "4gycb"

4. RESULTS AND DESCUSIONS

In their study, [13] propose an innovative security mechanism that integrates visual cryptography principles to reinforce CAPTCHA systems against sophisticated deep learning-based attacks. Their experimental results reveal a notable decrease in the attack success rate, dropping from 95% to approximately 53.83%, underscoring the efficacy of their approach. By leveraging visual cryptography the method introduces an additional layer of complexity that disrupts the ability of machine learning models to parse CAPTCHA content effectively. This deliberate obfuscation not only impedes automated recognition but also preserves human solvability, ensuring usability remains intact while significantly elevating security. The authors demonstrate that conventional deep learning models, which typically excel at pattern recognition, struggle to interpret the fragmented visual elements, thereby mitigating the risk of brute-force or algorithmic breaches.

Expanding upon this foundational work, our proposed methodology adopts a parallel strategy by implementing structurally modified CAPTCHAs designed to counteract automated exploitation. Similar to [13]'s framework, our enhancements focus on augmenting distortion techniques without compromising user accessibility. These modifications-ranging from dynamic noise injection to adaptive segmentation-are tailored to exploit the limitations of neural networks in processing discontinuous or cryptographically partitioned visual data. Empirical validations indicate that such refinements substantially improve resistance against evolving adversarial techniques, including generative adversarial networks (GANs) and reinforcement learning-based attacks. Consequently, our approach not only fortifies CAPTCHA durability but also aligns with the broader objective of sustaining human-centric authentication in an era of increasingly pervasive automation threats.

A critical consideration in this security framework is the necessity for the server to maintain a diverse repository of modified VCS combinations, as illustrated in Table 1. For example, a legitimate user response might follow the pattern "CAPTCHA-NOT CAPTCHA-NOT CAPTCHA-CAPTCHA", demonstrating the system's reliance on alternating valid and invalid segments. To operationalize this effectively, the server must store precomputed matrix representations for every possible response permutation, including but not limited to sequences like "CAPTCHA-CAPTCHA-NOT CAPTCHA-CAPTCHA" or "NOT CAPTCHA-CAPTCHA-NOT CAPTCHA-CAPTCHA". Each unique combination is mapped to a distinct matrix configuration, ensuring the

system can dynamically adapt to varying authentication requests. This design philosophy not only accommodates different interaction scenarios but also introduces an element of unpredictability that is crucial for thwarting automated attacks. By assigning specific matrices to each phase of the verification process, the system creates a multi-layered defense mechanism where the compromise of one authentication step does not inherently weaken subsequent stages.

The strategic deployment of multiple matrix combinations serves as a sophisticated countermeasure against adversarial exploitation. Attackers attempting to reverse-engineer or predict CAPTCHA responses face significant challenges due to the system's inherent variability—no single breach reveals the underlying structure of all possible combinations. This approach effectively mitigates the risk of pattern recognition algorithms successfully deciphering the authentication protocol, as each transaction presents a fresh cryptographic challenge. Moreover, the compartmentalization of matrix representations ensures that even if an attacker intercepts one segment of the communication, the remaining segments remain secure, preserving the overall system integrity. Such redundancy is particularly valuable in maintaining robust security postures against evolving threats, including machine learning-driven attacks that rely on consistent patterns. Ultimately, this methodology not only enhances the resilience of the CAPTCHA system but also aligns with broader cybersecurity principles that prioritize adaptive, layered defenses over static solutions.

Table 2. Average time required for solving CAPTCHA

CAPTCHA type	Mean
TEXT-based	21.33 s
IMAGE-based	23.51 s
Asirra	30 s
Our method	21 s

Recent studies in human-computer interaction (HCI) and cybersecurity have established that the average time required for users to solve conventional CAPTCHAs is approximately 21 seconds, as demonstrated in the empirical analyses conducted by [24], [25]. Building upon these findings, our proposed methodology incorporates a temporally staggered approach to CAPTCHA delivery, designed to optimize both security and usability. Specifically, we implement a standardized interval of 3 seconds between successive CAPTCHA transmissions, a duration calibrated to balance user convenience with the need to mitigate automated attacks. For instance, in a scenario involving the transmission of 7 distinct shares, the cumulative time from the initial to the final CAPTCHA would precisely align with the empirically observed 21-second benchmark (see Table 3). This synchronization ensures that the system remains consistent with established user response times while introducing a layered security mechanism.

The implementation of this temporally modulated framework offers two programmable configurations to accommodate varying operational requirements. The first approach adheres to a fixed 3-second interval between each share, ensuring predictability and ease of deployment. Alternatively, the system can be configured to dynamically dispatch subsequent CAPTCHAs immediately upon receiving the client response to the preceding one, thereby adapting to real-time user interaction patterns. However, to maintain the critical 21-second threshold—a duration validated by prior research as optimal for deterring bots without frustrating human users—the final (7th) CAPTCHA is deliberately timed to ensure the total process duration meets this benchmark. This flexibility in design not only enhances the system's adaptability to diverse use cases but also fortifies its resilience against brute-force attacks, as the variable timing disrupts predictable patterns that automated systems might exploit. By integrating these temporal controls, our method achieves a robust equilibrium between security efficacy and user experience, a balance underscored by its adherence to empirically validated timeframes.

Table 3. Temporal distribution of CAPTCHA shares

Process stage	Time elapsed (seconds)
Initial CAPTCHA (Share 1)	0
Share 2	3
Share 3	6
...	...
Final CAPTCHA (Share 7)	21

To evaluate the security of this method in comparison to existing approaches, the probability of successfully deciphering this sequence of 7 CAPTCHAs is $(\frac{1}{2})^7$, which is approximately equal to 0.0078. This implies that within 5.8 hours, this combination of 7 CAPTCHAs could be cracked 7.8 times, which is equivalent to a single CAPTCHA being solved every 44.8 minutes. To wrap up, this approach works well in this scenario, as it strikes a balance between strong security and user convenience. By carefully designing the system to limit automated attacks and ensuring reasonable response times, it effectively protects against unauthorized access. The results highlight its practicality and reliability, making it a solid choice for the task at hand.

5. CONCLUSION

In conclusion, the novel authentication method, which integrates an advanced form of visual cryptography, provides a significantly stronger defense against automated attacks, thereby enhancing security when compared to traditional CAPTCHA systems. This approach not only addresses the growing threats posed by deep learning techniques, which have been successful in bypassing standard CAPTCHA challenges, but it also improves the overall user experience. By optimizing the process, it adapts the time and effort required from users to complete the authentication, making it effective and more accessible. Furthermore, the method enhances operational efficiency, enabling seamless interaction without compromising security. As a result, this authentication scheme presents a compelling alternative to current CAPTCHA solutions, offering a well rounded balance between robust, high level security and a user friendly interface, ultimately creating a more effective and practical solution for modern applications.

ACKNOWLEDGEMENTS

The authors wish to thank the editors and anonymous reviewers for their generous time and insightful critiques. Their expert guidance helped shape stronger arguments and improved the manuscript's organization and readability.

REFERENCES

- [1] M. Moradi and M. Keyvanpour, "CAPTCHA and its alternatives: a review," *Security and Communication Networks*, vol. 8, no. 12, pp. 2135–2156, Aug. 2015, doi: 10.1002/sec.1157.
- [2] C. Pope and K. Kaur, "Is it human or computer? Defending e-commerce with captchas," *IT Professional*, vol. 7, no. 2, pp. 43–49, Jan. 2005, doi: 10.1109/MITP.2005.37.
- [3] A. S. Almazayad, Y. Ahmad, and S. A. Kouchay, "Multi-modal CAPTCHA: a user verification scheme," in *2011 International Conference on Information Science and Applications*, Apr. 2011, pp. 1–7, doi: 10.1109/ICISA.2011.5772421.
- [4] V. D. Nguyen, "Contributions to text-based CAPTCHA security," *University of Wollongong*, p. 190, 2014.
- [5] A. E. Ali, N. F. Hassan, and M. E. EL-Deen Abdulmunim, "Generate animated CAPTCHA based on visual cryptography concept," *Engineering and Technology Journal*, vol. 29, no. 16, pp. 3405–3416, Dec. 2011, doi: 10.30684/etj.29.16.12.
- [6] I. E. Olufemi, A. A. Adebisi, F. A. Ibikunle, M. O. Adebisi, and O. O. Oludayo, "Research trends on CAPTCHA: a systematic literature," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 5, pp. 4300–4312, 2021, doi: 10.11591/ijece.v11i5.pp4300-4312.
- [7] M. Kumar, M. K. Jindal, and M. Kumar, "A systematic survey on CAPTCHA recognition: types, creation and breaking techniques," *Archives of Computational Methods in Engineering*, vol. 29, no. 2, pp. 1107–1136, Mar. 2022, doi: 10.1007/s11831-021-09608-4.
- [8] M. Kumar and M. K. Jindal, "Benchmarks for designing a secure devanagari CAPTCHA," *SN Computer Science*, vol. 2, no. 1, p. 45, Feb. 2021, doi: 10.1007/s42979-020-00445-z.
- [9] M. Kumar, M. K. Jindal, and M. Kumar, "Design of innovative CAPTCHA for hindi language," *Neural Computing and Applications*, vol. 34, no. 6, pp. 4957–4992, Mar. 2022, doi: 10.1007/s00521-021-06686-0.
- [10] M. Kumar, M. K. Jindal, and M. Kumar, "A novel attack on monochrome and greyscale devanagari CAPTCHAs," *ACM Transactions on Asian and Low-Resource Language Information Processing*, vol. 20, no. 4, pp. 1–30, Jul. 2021, doi: 10.1145/3439798.
- [11] M. Kumar, M. K. Jindal, and M. Kumar, "An efficient technique for breaking of coloured Hindi CAPTCHA," *Soft Computing*, vol. 27, no. 16, pp. 11661–11686, Aug. 2023, doi: 10.1007/s00500-023-07844-3.
- [12] M. Naor and A. Shamir, "Visual cryptography," in A. De Santis, *Advances in Cryptography EUROCRYPT, LNCS, Springer, Berlin*, 1995, pp. 1–12.
- [13] X. Yan, F. Liu, W. Q. Yan, and Y. Lu, "Applying visual cryptography to enhance text captchas," *Mathematics*, vol. 8, no. 3, p. 332, Mar. 2020, doi: 10.3390/math8030332.
- [14] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, no. 2, pp. 86–106, Sep. 1996, doi: 10.1006/inco.1996.0076.
- [15] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes, and Cryptography*, vol. 11, no. 2, pp. 179–196, 1997, doi: 10.1023/A:1008280705142.
- [16] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoretical Computer Science*, vol. 240, no. 2, pp. 471–485, Jun. 2000, doi: 10.1016/S0304-3975(99)00243-1.

- [17] A. Adhikari, "Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images," *Designs, Codes and Cryptography*, vol. 73, no. 3, pp. 865–895, Dec. 2014, doi: 10.1007/s10623-013-9832-5.
- [18] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010, doi: 10.1109/TIFS.2009.2037660.
- [19] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM Journal on Discrete Mathematics*, vol. 16, no. 2, pp. 224–261, Jan. 2003, doi: 10.1137/S0895480198336683.
- [20] H. Koga, *Advances in Cryptology — ASIACRYPT 2002*, vol. 2501. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002.
- [21] H. Koga and E. Ueda, "Basic properties of the (t, n) -threshold visual secret sharing scheme with perfect reconstruction of black pixels," *Designs, Codes and Cryptography*, vol. 40, no. 1, pp. 81–102, Jul. 2006, doi: 10.1007/s10623-005-6700-y.
- [22] M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," *Combinatorics, Probability and Computing*, vol. 12, no. 3, pp. 285–299, May 2003, doi: 10.1017/S096354830200559X.
- [23] M. Bose and R. Mukerjee, "Optimal (k, n) visual cryptographic schemes for general k ," *Designs, Codes and Cryptography*, vol. 55, no. 1, pp. 19–35, Apr. 2010, doi: 10.1007/s10623-009-9327-6.
- [24] A. Adesina, P. Ayobioloja, I. Obagbuwa, T. Odule, A. Afolorunso, and S. Ajagbe, "An improved text based and image-based captcha based on solving and response time," *Computers, Materials and Continua*, vol. 74, no. 2, pp. 2661–2675, 2022.
- [25] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: a captcha that exploits interest-aligned manual image categorization," in *Proceedings of the 14th ACM conference on Computer and communications security*, Oct. 2007, pp. 366–374, doi: 10.1145/1315245.1315291.

BIOGRAPHIES OF AUTHORS



Chihi Hasnae    is an engineer and doctoral candidate, holds an engineering degree in Computer Science from National School of Applied Sciences (ENSA) in Tangier, awarded in 2022. She is currently pursuing a Ph.D. in Computer Science at the same institution, under the supervision of the MASI team. Her research focuses on information systems, cybersecurity, and databases, with a particular interest in enhancing the security and performance of modern data driven applications. Through her academic work, she aims to contribute to the advancement of efficient and secure systems in the field of computer science. She can be contacted at email: chihi.hasnaa@gmail.com.



Chahboun Asaad    is a distinguished expert with an extensive educational background in Telecommunications. He earned both his Master of Science (M.S.) and Doctor of Philosophy (Ph.D.) degrees in Telecommunications from Abdelmalek Essaadi University in the UAE, and an Engineer degree from the Central School of Arts and Businesses in Brussels, Belgium. He has a diverse work experience, which includes responsible engineer of radiology, working as a Maintenance and medical imaging materials in Rabat, Morocco. Currently, he is the head of the MASI research team in the Information Systems and Communication Department at the National School of Applied Sciences in Tangier, Morocco, at the University of Abdelmalek Essaadi. As a researcher, his focus is on several areas of interest, including wireless routing in Ad-hoc networks, sensor networks, network security, IoT, the development of remote sensing methods for land cover dynamic monitoring, grid computing and remote sensing. He can be contacted at email: achahboun@uae.ac.ma.